REMARKS

Claims 1-3 and 5-36 are all the claims presently pending in the application.

Claim 7 is amended merely to clarify the features of the invention and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicants specifically state that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1-3 and 5-36 stand rejected on prior art grounds. Claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Borza (U.S. Patent No. 6,446,210). Claims 5-8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza. Claims 10-13, 19, 21-23, 29, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza and further in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention relates to a method of processing semiotic data.

In an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of processing semiotic data includes receiving semiotic data including a data set P, selecting a function h, and for at least one of each the data set P to be collected, computing h(P), destroying the data set P, storing h(P) in a database, and to determine whether P' is a predetermined subject, comparing h(P') to available h(P)s to determine whether there is a match, wherein the data set P cannot be extracted from h(P).

In another exemplary embodiment of the invention, as defined by independent claim 5, a method of processing semiotic data includes receiving semiotic data including a data set P, selecting a function h, and for at least one of each the data set P to be collected, computing h(P), destroying the data set P, and storing h(P) in a database, wherein the data set P cannot be extracted from h(P). The method further includes selecting a private key/public key (K, k) once for all cases, and one of destroying the private key K and sending the private key K to a trusted party, and choosing the function h as the public encryption function corresponding to k.

In another exemplary embodiment of the invention, as defined by independent claim 9, a method of processing semiotic data includes receiving semiotic data including a data set P, selecting a function h, and for at least one of each the data set P to be collected, computing h(P), destroying the data set P, and storing h(P) in a database, wherein the data set P cannot be extracted from h(P), wherein the data set P is not determined perfectly by its reading, wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of the initial reading is stored after further processing thereof, wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data.

In another exemplary embodiment of the invention, as defined by independent claim 15, a method of processing biometric data includes acquiring unencrypted biometric data including at least one data set P, encrypting, with one of a secure hash function and an identity function, each the at least one data set acquired, destroying the unencrypted data set P, storing each of the at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from the data stored in the database, and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match.

In another exemplary embodiment of the invention, as defined by independent claim 17, a method of extracting components of biometric data which are stable under measurement errors includes destroying the unencrypted data set P, storing each the at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from the data stored in the database, and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match.

In another exemplary embodiment of the invention, as defined by independent claim 19, a method of extracting components of biometric data which are stable under measurement errors includes destroying the unencrypted data set P and storing each the at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from the data stored in the database, extracting sub-collections Sj from the collection of data in the data set P, and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

Independent claims 24, 27, 29, 31, 33, and 35 recite somewhat similar novel and unobvious combinations of elements.

For example, in another exemplary embodiment of the invention, as defined by independent claim 24, a system for processing semiotic data includes means for destroying the data set P and means for comparing h(P') to available h(P)s to determine whether there is a match.

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

II. PRIOR ART REJECTIONS

A. Claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36 stand rejected under 35 U.S.C. §102(e) as being anticipated by Borza. Applicants submit, however, that there are elements of the claimed invention which are neither taught nor suggested by Borza, and therefore, Applicants respectfully traverse this rejection.

For example, independent claim 1 recites a method of processing semiotic data, comprising:

> selecting a function h, and for at least one of each said data set P to be collected, computing h(P);
> destroying said data set P;
> storing h(P) in a database, and
> to determine whether P' is a predetermined subject, comparing h(P') to available h(P)s to determine whether there is a match,
> wherein said data set P cannot be extracted from h(P)
> (emphasis added).

In an exemplary embodiment of the present invention, when authenticating a piece of biometric data, an encrypted (or otherwise modified) version of the data is compared with the encrypted data in the database. This preserves privacy, as the unencrypted biometric data is not used by the computer in the authentication process but, instead, the encrypted data is used.

That is, in the claimed invention, the data that is stored and compared is not the biometric data P itself, but instead, is an encrypted version h(P).

In comparison, while Borza generally describes comparing the encrypted data against an encrypted template (see Borza at column 8, lines 28-38), Borza simply appears to mention this only a single time in the disclosure and does not elaborate on this feature again. That is, Borza does not disclose or suggest with sufficient specificity how such a comparison could be implemented or accomplished.

Indeed, Applicants respectfully submit that the method described by Borza could not work in general, since such a comparison would generally be based on comparing matching scores and, because encryption diffuses the data, such comparison against the scores of encrypted data would not work (e.g., without significantly altering the accuracy and sensitivity of the identification process).

Specifically, a new data P' is matched against data P in the database if P' is "close" to P. However, the diffusive nature of encryption would ensure that h(P) would be far from h(P'). Thus, Applicants respectfully submit that it would not be possible to match h(P) against h(P').

On the other hand, the claimed invention provides specific solutions to this problem (e.g., see specification at pages 17-20) and defined by novel and unobvious combination of elements recited in claims 1-3 and 5-36.

Accordingly, Applicants respectfully submit that Borza neither discloses nor suggests at least "comparing h(P') to available h(P)s to determine whether there is a match", in as complete detail as recited, for example, in independent claim 1.

Thus, for the foregoing reasons, Applicants respectfully submit that Borza neither discloses nor suggests all of the features of claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36, and therefore, respectfully requests that the Examiner with draw this rejection.

B. Claims 5-8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza.

Applicants respectfully submit that claims 5-8 are patentable over Borza for somewhat similar reasons as those set forth above.

Moreover, with respect to claim 5, the Examiner acknowledges that Borza does not disclose or suggest destroying the private key K and sending the private key K to a trusted party. However, the Examiner alleges that if would have been obvious to destroy the private key K and send the private key to a trusted third party, since it allegedly is known in the art that the private key is needed to decrypt any message encrypted with the public key k, and therefore, the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k.

Applicants respectfully submit that, assuming *arguendo* that it is known in the art that the private key is needed to decrypt any message encrypted with the public key k and that the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k, it would not have been obvious to modify Borza to arrive at the claimed combination of features recited in the claimed invention.

For example, Borza merely relates to a method for enhancing network security for a communication session initiated between a first computer and a second computer (e.g., see Borza at Abstract).

On the other hand, the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, <u>without significantly altering the accuracy and sensitivity of the identification process</u> (e.g., see specification at page 3, lines 9-14).

As described in an illustrative embodiment of the invention, for each P to be collected, h(P) is computed, P is destroyed, and h(P) is stored in a database (e.g., see specification at page 14, lines 10-11). In the claimed invention, the private key K is maintained, if at all, only by a trusted third party (e.g., the Supreme Court, the FBI, etc.) and P cannot be extracted from h(P) except by the trusted party (e.g., see specification at page 14, lines 7-15). Otherwise, h(P') is compared to all available h(P)s to determine if one of them matches, as recited, for example, in claim 7.

Thus, Applicants respectfully submit that Borza neither discloses nor suggests all of the features of claims 5-8, and further, that it would not have been obvious to modify Borza to arrive at the claimed combination of features recited in the claimed invention.

Accordingly, Applicants respectfully request that the rejection of claims 5-8 be withdrawn.

C. Claims 10-13, 19, 21-23, 29, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza and further in view of Kharon.

Applicants respectfully submit that claims 10-13, 19, 21-23, 29, and 35 are patentable over Borza for somewhat similar reasons as those set forth above with respect to, for example, independent claim 1.

On the other hand, Kharon does not make up for the deficiencies of Borza, and therefore, independent claims 1, 9, 19, 29, or 35 would not have been obvious over Borza or Kharon, either alone or in combination. Indeed, the Examiner does not even rely on Kharon for the disclosure of such features, as mentioned above.

Moreover, claims 10-13, 19, 21-23, 29, and 35 also are patentable over Borza or Kharon, either alone or in combination, by virtue of the additional, novel and unobvious combination of features recited therein.

For example, with respect to claim 10 (see Office Action, numbered paragraph 23), while Kharon appears to describe how minutia in fingerprints are compared, Kharon does not describe the claimed method of computing subcollections and encrypting them (see Kharon at column 13, lines 43-67).

In comparison, a novel and unobvious aspect of the claimed invention is not merely to use a smaller data set, but to use many smaller subsets of the original data set and encrypting such smaller subsets of the original data set.

As with Borza, in Kharon, unencrypted minutiae data must be compared, since the encryption would diffuse the data, and therefore, would render comparison against a threshold impossible (e.g., see Kharon at column 14, lines 28-39, and column 15, lines 42-55).

As another example, with respect to claims 12 and 23 (e.g., see Office Action, numbered paragraph 26), while Borza appears to describe the possibility of false rejection, Borza does not teach or suggest that the computation of the variations is possible with a particular piece of biometric data (e.g., see Borza at column 11, lines 25-34).

Similarly, Borza also does not teach or suggest the computation of variations (e.g., see Borza at column 12, lines 25-61).

Further, while Borza appears to describe encrypting the data before transmission, Borza does not describe comparing encrypted data against encrypted data in the database (e.g., see Borza at column 12, lines 25-61).

Also, while Borza appears to describe how multiple biometric data can be used to authenticate a person, Borza does not address how to compare encrypted data. (e.g., see Borza at column 11, line 65 to column 12 line 34).

Thus, for the foregoing reasons, Applicant respectfully submit that neither Borza nor Kharon discloses or suggests all of the features of claims 10-13, 19, 21-23, 29, and 35, and therefore, requests that the Examiner withdraw this rejection of claims 10-13, 19, 21-23, 29, and 35.

III. CONCLUSION

In view of the foregoing, Applicant submits that claims 1-3 and 5-36, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: JUNE 18, 2004

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (703) 872-9306 the enclosed Amendment under 37 C.F.R. § 1.111 to Examiner Christian A. La Forgia on June 18, 2004.

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386